2019 NSF Community Cybersecurity Benchmarking Survey Report

10 Jan 2020

For Public Distribution

Scott Russell,[1] Kelli Shute

[1] Project Lead, scolruss@indiana.edu

About the NSF Cybersecurity Center of Excellence

Our mission is to provide the NSF community a coherent understanding of cybersecurity's role in producing trustworthy science and the information and know-how required to achieve and maintain effective cybersecurity programs.

Acknowledgments

The authors thank Von Welch, Jim Marsteller, and the members of the Trusted CI team who participated in the development and socialization of the survey, and to all other team and community members who contributed ideas regarding the content of the survey. Special thanks go to Von Welch, Mark Krenz, Bob Cowles, and Kathy Benninger for their help in reviewing and refining the analysis.

Many thanks to all the respondents.

This document is a product of Trusted CI. Trusted CI is supported by the National Science Foundation under Grants Number ACI-1547272. For more information about the Trusted CI please visit: https://trustedci.org/. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Using & Citing this Work

Table of Contents

Executive Summary

The purpose of this survey is to collect, analyze, and publish useful baseline benchmarking information about the NSF science community's cybersecurity programs, practices, challenges, and concerns. We received 23[2] responses to this year's survey, including 19 from respondents with annual budgets greater than $1M, and 14 from NSF Major Facilities. The mean total budget of respondents was $30,800,000 and the median budget was $22,000,000. This was the third year of the NSF Community Cybersecurity Benchmarking Survey. Highlights from the results and findings include the following:

A. Respondents' cybersecurity budgets continue to vary widely, with Major Facilities having budgets ranging from 1% to 25% of IT budget, with a mean of 7.5%. This is a slight increase in cybersecurity spending from 2017, which had a range of 0.2% to 26% of IT budget, with a mean of 6.8%.
B. 4 of the 14 Major Facility respondents did not provide a discrete cybersecurity budget or had a budget of $0. This is largely the same as the 2017 survey (4 of 15 Large Facility respondents).
C. 11 of 23 respondents claimed their organization has dedicated adequate resources (e.g. budget, personnel, tools) to their cybersecurity program. 7 respondents claimed their organization has not dedicated adequate resources, and 5 responded "not sure." Interestingly, 3 respondents who felt their cybersecurity program had adequate resources did not provide a cybersecurity budget.
D. All respondents either have a cybersecurity program (16) or are in the process of establishing one (7).
E. 15 of 23 respondents have a CISO or equivalent role (8 full-time; 7 part-time). This is down from 2017, where 16 of 20 respondents had CISOs. However, the number of full-time CISOs increased, from 4 of 20 in 2017 to 8 of 23 in 2019. 10 of 14 Major Facilities have a CISO (3 full-time; 7 part-time). This is comparable to 2017, where 12 of 15 LFs had CISOs (2 full-time; 10 part time).
F. 21 respondents have cybersecurity full-time employees (FTEs) (including partial FTEs). 10 have the equivalent of one cyber FTE or greater. This is comparable to 2017, where 19 of 20 respondents identified some level of cyber FTE effort, with 8 having the equivalent of one cyber FTE or greater.
G. The large majority of respondents authenticate users from multiple institutions, with 14 authenticating from more than 3 external sites, and 20 authenticating from at least 2.
H. 17 of 23 (~75%) respondents use multi-factor authentication. This continues the trend of increasing adoption of MFA, from 6 out of 27 (22%) in 2016, to 12 out of 20 (60%) in 2017.
I. Residual risk acceptance is widely practiced, with Senior Management of Principle Investigators as the most common risk acceptor. 3 respondents had no process for residual risk acceptance. This is a significant change from 2017, where 9 of 20 respondents had no process for residual risk acceptance.
J. The most commonly cited control sets were NIST 800-171 (5) (despite only 2 handling CUI), the CIS controls (4), and FISMA low/moderate (4). 5 respondents had not selected a baseline control set.
K. 16 of 23 respondents develop and adopt cybersecurity policies, but 7 of those respondents explicitly acknowledge that they do not properly follow and enforce their own policies.
L. The most common cybersecurity requirements arose from NSF Cooperative Agreements (13), State PII laws (11), and non-disclosure agreements (8).
M. 21 of 23 respondents develop software, including all 14 Major Facilities. 1 respondent develops in only compiled languages, 4 only in interpreted languages, and 16 develop in both.
N. Coding practices were widely practiced. The least common coding practices were static and dynamic analysis (4), code signing (4), and automated documentation tools (6).
O. Patching times are highly variable, with critical patches ranging from 2 days up to a month to implement.
P. 4 of 23 respondents detected 3 or more incidents, and 9 detected at least one incident.

[2] Note, we do not track the extent to which the current years' respondents overlap with previous years' respondents.

1 Introduction

Benchmarking information is frequently used to develop a common sense of status and norms within a community or sector. At the 2015 NSF Cybersecurity Summit, the audience indicated that there was interest in generating a survey of the state of cybersecurity for the NSF science community, and that the community would respond to the survey and utilize the results. Based on this positive feedback, Trusted CI established the Community Survey project, and conducted its first annual community survey in 2016. This is the third Community Survey report.

The purpose of Trusted CI's Community Survey project is to collect, analyze, and publish useful baseline benchmarking information about the NSF science community's cybersecurity programs, practices, challenges, and concerns.

The remainder of this report is as follows: Section 2 describes the methodology for constructing the survey and collecting responses; Section 3 presents an overview of the survey data collected; Section 4 provides our analysis of the survey data; and Section 5 concludes with broader reflections.

2 Methodology

In this section, we describe our target respondent community, target audience for this report, survey construction, and response collection.

2.1 Responding Community and Audience

2.1.1 NSF Project Community

NSF awards approximately 27% of the total federal budget for basic research, supporting over 350,000 researchers, post-doctoral fellows, trainees, teachers, and students.[3] Among the NSF's active awards are 20 NSF Major Facilities (MF), previously referred to as Large Facilities.[4] This survey was targeted to the NSF community of science projects and facilities.

2.1.2 Audience for This Report

We envision three primary audiences for this report:

- NSF-funded science projects and facilities. The survey results may assist large science projects and facilities in developing a sense of norms and practices in the community.
- NSF leadership and program officers. The survey results may give NSF leadership and program officers greater insight into norms and practices in the community.
- Trusted CI. The survey results will assist Trusted CI in tailoring its services to the current state of cybersecurity at NSF-funded projects and facilities.

[3] https://www.nsf.gov/news/news_summ.jsp?cntn_id=100595

[4] *See* https://www.nsf.gov/bfa/lfo/docs/major-facilities-list.pdf. Note, Major Facilities are broken down into 20 programs, with 12 subprograms.

2.2 Survey Construction

We designed survey questions to collect information on respondents' budgets and other descriptive attributes relevant to cybersecurity, including information on specific cybersecurity practices, events, and concerns. From Nov. 6, 2018 through Jan. 4, 2019, we took proposals from Trusted CI to improve the survey. A text copy of the survey is included as Appendix A.

Response to this survey was voluntary and optional. To encourage a higher response rate and more complete responses, we purposely avoided collecting project identifying information, such as project names or award numbers. Responses were collected using Google Forms.

2.3 Response Collection

The survey was announced on May 23, 2019 on the Trusted CI "Announce" mailing list. The survey was further promoted on Trusted CI's Blog on July 3, 2019, through the XSEDE mailing list, and during the Large Facility Security Team meetings during the months of May, June, and July. Reminders were posted to the Trusted CI Announce email list on July 18, July 29, and July 31. The response period to the survey closed on July 31, 2019.

2.4 Response Evaluation

Responses were evaluated at face value, despite some responses falling far outside of expected ranges. Averages were calculated based solely on non-null/non-zero responses in calculating average; including null/zero responses in the budget averages would have skewed the results and led to misleading averages.

The responses were compiled in a spreadsheet, with questions broken down to represent each possible answer when multiple answers were allowed, and with additional space for calculated answers, such as the respondent's cybersecurity budget as a percentage of IT budget. This spreadsheet was utilized to develop a preliminary analysis of the results, culminating in the development of a Preliminary Findings document that was circulated on the Trusted CI team listserv on Oct 7, 2019.

3 Results

Below, we provide a high level picture of the response rates and the categories of respondents that emerged in this response group.

3.1 Response Rates

The survey received 23 responses. In light of the thousands of active NSF awards, we caution against any conclusion that these results are representative of the community at large. However, we received responses from 14 NSF Major Facilities, plus 5 additional responses from awards with annual budgets greater than $1,000,000.

3.2 Response Categorization

Using the methodology set out from the 2016 survey,[5] we continued to group the respondents by annual budget, with the three categories consisting of: 1. **Major Facilities** (15) - a specific designation by NSF; 2. **Big** (3) - respondents with annual budgets over $1M; and 3. **Small** (1) - respondents with annual budgets under $1M. Considering the high relative response rate of Major Facilities on this year's survey (15 out of the 20 respondents), our analysis is primarily related to the cybersecurity of Major Facilities, but does include a discussion of the other, non-MF respondents.

4 Analysis

In this section, we provide high level analysis of the survey responses, highlighting results that were particularly interesting, unexpected, notable, or concerning. Additionally, we compare the results to past years' surveys, and highlight any trends or deviations we find.[6] Considering the majority of respondents were Major Facilities, our analysis is largely focused on the security implications for Major Facilities. The relevant survey question is denoted with a letter-number pair in square brackets (e.g., [Q6]) (for the full question text, see Appendix A).

4.1 Project or Facility Budget

Respondents were asked to provide the annual budget [Q3], the annual IT budget [Q4], and the annual cybersecurity budget [Q5] for their project or facility. Annual budgets among the Major Facilities ranged from $1M to $100M, with a mean of $43M and median of $38M.[7] Despite this already significant variation in total budgets, cybersecurity budgets among the respondents varied considerably, with 4 Major Facilities not being able to provide a cybersecurity budget, and others as low as $1000, while at the high end cybersecurity budgets reached $1.3M. Similar to past years, this variability seemed to increase when controlling for IT budget, with MF's cybersecurity budgets ranging from 1% to 25% of IT budget. Among all respondents, the median cybersecurity budget as a percentage of IT budget was 5%, and the mean was 7.5%. Notably, this falls within the normal range across a number of industries.[8]

As found in previous years, one potential explanation for the variability in cybersecurity budgets is the lack of uniformity in what costs are included in the cybersecurity budget. Among organizations with cybersecurity budgets, 5 did not include labor, 2 did not include hardware, and 5 did not include software [Q6].

---

[5] Note, the methodology has updated from "Large Facilities" to "Major Facilities," in keeping with NSF classification.
[6] Note again that we do not track overlap in respondents between years.
[7] These numbers were slightly lower than 2017, which ranged from $8M to $100M, with a mean of $45M and median of $40M.
[8] *See, e.g.*, Scott Russell, Craig Jackson, Robert Cowles, Cybersecurity Budgeting: A Survey of Benchmarking Research and Recommendations to Organizations, presented at and published in the report of the 2016 NSF Cybersecurity Summit, Arlington, VA, 17 Aug 2016.

	MF category	Overall
Cybersecurity as % of Annual Budget (non-zero mean value)	0.51%	0.56%
Cybersecurity as % of Annual Budget (non-zero range)	0.01% - 1.39%	0.01% - 1.39%
Cybersecurity as % of IT Budget (non-zero mean value)	7.9%	7.5%
Cybersecurity as % of IT Budget (non-zero range)	1% - 25%	1% - 25%

Finally, a new question in the 2019 survey asked respondents whether they felt their organization has devoted adequate resources (e.g., budget, personnel, tools) to their cybersecurity program [Q7]. 11 of 23 respondents claim their organization has dedicated adequate resources to their cybersecurity program. 7 respondents claimed their organization has not dedicated adequate resources, and 5 responded "not sure." Interestingly, 3 respondents who indicated "yes" did not have a cybersecurity budget, whereas the respondent with the highest cybersecurity budget (in dollars) indicated that they did not have adequate resources. Notably, respondents who did not employ a CISO were much more likely to feel that they did not have adequate resources or would be uncertain (6 of 8). The inverse appears to not be true, however, as respondents with a CISO were not more likely to believe they had adequate resources than that they did not have adequate resources.

4.2 Project or Facility Attributes

Survey questions in this group were meant to uncover information about the environment in which cybersecurity takes places.

4.2.1 Nearly all respondents had complex authentication environments, with 20 of 23 accommodating users from multiple external institutions [Q6] and 14 indicating a need to authenticate from more than three external institutions. These responses were largely irrespective of annual budget, with 6 non-Large Facilities authenticating from more than three external locations, and one Large Facility not authenticating from any external locations. These results largely mirror those from previous surveys. Future surveys may benefit from clarifying the types of locations that are being authenticated from (e.g. multiple facilities controlled by the same entity; employees working from home; third parties seeking access to facility resources; etc.)

4.2.2 The role of cybersecurity officers, (such as a CISO, ISO, or CSO), varied greatly among the respondents as well (Q8]. The majority of respondents had a cybersecurity officer (15 of 23; 10 of 14 Major Facilities), of which 8 were full-time and 7 were part-time. Although this is a lower percentage of respondents with a CISO from 2017 (16 of 20 in 2017 vs. 15 of 23 in 2019), the percentage of respondents with a full-time CISO notably increased (from 4 of 16 to 8 of 15). However, as with

previous years, the practice of employing a CISO appears to be fairly erratic. For instance, the respondent with the largest cybersecurity budget as a percentage of IT budget (25%) did not employ a CISO, whereas 5 respondents employed a CISO without having a cybersecurity budget. Moreover, 7 respondents that do not have a CISO still employ cybersecurity FTEs, whereas 1 respondent had a full-time CISO with no cybersecurity FTEs. This variability in cybersecurity leadership practices is hard to reconcile, and indicates that cybersecurity governance is not consistently practiced across facilities.

4.2.3 Cybersecurity Full Time Employees (FTEs) [Q9] roughly tracked with cybersecurity budgets, excepting those respondents who did not include labor in their budget calculations [Q4]. The clear majority employ at least a partial cybersecurity FTE (22 of 24). However, over half of all respondents (14/24) employ the equivalent of 1 cyber FTE or less.

4.2.4 21 out of 24 respondents developed or maintained software in house [Q9]. Of those who did, 16 used both interpreted and compiled languages. All 14 Major Facilities queried developed and maintained software, of which 10 used both interpreted and compiled languages, 1 used only compiled languages, and 3 used only interpreted languages. Of the queried coding practices, Source Code Repositories (18), Coding Standards (15), Issue Tracking/Vulnerability Management (13), and Continuous Integration (13) were the most widely practiced, whereas Static and Dynamic Analysis (4), Code Signing (5), and Automated Documentation Tools (4) were the least frequently adopted. These results largely mirror those from previous surveys.

4.3 Cybersecurity Programs and Practices

4.3.1 All of the respondents have either already established a cybersecurity program (16) or are in the process of establishing a cybersecurity program (7) [Q13]. Most institutions engage their leadership in cybersecurity decision making either yearly or quarterly (7 of 23 each) [Q15]. Whereas the majority of risks are accepted by Senior Managers or PIs (14) or by IT managers (8) [Q22]. (Note, this is a dramatic increase from previous years; in 2017, nearly half of all respondents had no process for risk acceptance, compared to only 3 respondents with no process in 2019.) Notably, nearly half of respondents identified multiple roles that accept risk (11 of 23), suggesting that risk acceptance is distributed throughout the organization.

4.3.2 The most widely used role for policy development was an IT or cyber manager (13 of 16) [Q16]. However, a number of facilities or projects identified multiple organizational elements that participate in policy development, with 8 also using a Governance Board. (Interestingly, only one respondent *only* utilized a governance board). Additionally, 10 respondents relied on their parent institution for some portion of policy development. 3 respondents had no process for policy development.

4.3.3 Nearly all respondents have policies covering system operators and users (19 of 23) [Q14], whereas a majority of respondents have policies that cover leadership, owners, and third parties (14

of 23). The largest policy blind spot identified was covering vendors, which only 7 respondents have policies for. Notably, 7 respondents explicitly acknowledge that they do not adequately follow and enforce the policies they create [Q17].

4.3.4 Over half (13 of 23) of respondents utilize a baseline control set [Q18].[9] Of those that do, the most commonly utilized are NIST 800-171 (5), the CIS Controls (4), and FISMA Low/Moderate (4). Interestingly, roughly half of respondents have no process for selecting additional[10] (11) or alternate[11] controls (12). This suggests that institutions may need assistance in tailoring generic guidance for the specific needs of their organization and mission.

4.3.6 The majority of respondents utilized additional cybersecurity frameworks and guidance (15 of 23) [Q19]. The most popular frameworks were the Trusted CI Guide (8 of 23), NIST Cybersecurity Framework (4 of 23), and NIST Risk Management Framework (3 of 23). Interestingly, these numbers are universally lower than in previous years. This may be do to updates in this year's survey structure that distinguishes "Baseline Control Sets" from "Cybersecurity Frameworks," which are often used (erroneously) interchangeably. More guidance on this topic could be valuable to the community.

4.3.7 Nearly all respondents are subject to external cybersecurity requirements (20 of 23) [Q23], with the terms of their cooperative agreement being the most common (13 of 23).[12] Personally Identifiable Information (11), Protected Health Information (6), and Non-Disclosure/Contractual Agreements (8) were also fairly common.[13] Interestingly, only 2 respondents are subject to Controlled Unclassified Information (CUI) requirements, despite NIST's CUI baseline control set (SP 800-171) being the most commonly utilized baseline control set identified in Question 18.

4.3.8 Programmatic safeguards were overall more widely adopted than in previous years [Q25], with 16 respondents implementing an overarching cybersecurity strategy, 16 having documented cybersecurity standards, 14 adopting a specific incident response policy, 14 utilizing a business continuity plan, 14 utilizing an inventory, 14 reviewing security intelligence products, and 13

[9] A "baseline control set" is a predetermined set of security controls used as a default for organizations when selecting security controls for their assets. Examples of baseline control sets include: the CIS Controls, the ASD Essential Eight, and FISMA Moderate (via NIST SP 800-53).

[10] Additional controls are "controls selected beyond those specified in the baseline control set. Reasons for selecting an additional control include: to address a particularized threat; to address an unacceptable risk; to satisfy a compliance requirement; or to satisfy a contractual obligation."

[11] Alternate controls are "controls selected instead of controls in the baseline control set. Reasons for selecting an alternate control in place of a baseline control include: improves employee quality of life; better addresses the organization's operating environment; better addresses the organization's unique risk profile; or the baseline control was too costly to implement."

[12] Note, that all Large Facilities are subject to cooperative agreement terms, so at least one Large Facility is not aware of the cybersecurity requirements listed in their CA. Additionally, two respondents identified both "none" and "cooperative agreement terms from NSF," suggesting some potential confusion.

[13] One respondent wrote in the European Union's General Data Protection Regulation (GDPR), which was not presented as an option. This will be updated for future Surveys.

adopting roadmaps to implement cybersecurity improvements. Maturity Models (4), Information Security Governance structures (7), risk assessments (10), and external reviews (10) were the least commonly practiced.

4.3.9 A subset of operational safeguards [Q26] are widely adopted, such as firewalls (22), physical access control (19), central logging (18), anti-virus (15), and vulnerability management (14). Practices with the lowest adoption rates are live exercises (3), real time alerts (4), penetration testing (6), and table top exercises (7).

4.3.10 Multi-factor authentication (MFA) is adopted by 17 of the 23 respondents. This continues a trend of increasing adoption of MFA, from 22% in 2016 to 60% in 2017 to 74% in 2019. Consistent with this trend, only 4 of 14 Major Facilities are currently not using MFA, down from 7 of 15 in 2017 and 7 of 9 in 2016.

4.3.11 Patching times continue to vary greatly between respondents, and even within respondents depending on the criticality of the patch [Q27]. For critical patches, respondents' response times range from 2 days to >3 months to implement, with the most common answers being 2 days (9) and 1 week (8). (This is an incremental improvement from 2017, where 1 week was the most common response, and 2 days was second.) Outside of critical patches, response times vary more widely. Most organizations manage "important" patches at one timescale slower than critical patches (e.g. 2 days → 1 week; 1 week → 1 month). Unlike in previous years, however, most respondents did not treat all non-critical patches uniformly (i.e. important, moderate, and low all addressed in the same time period.) Instead, most respondents implement a response time commensurate with the patch's criticality, with less critical patches being addressed over longer periods of time.

4.3.12 Incident tracking was down from 2017, with 9 of 23 respondents detecting at least one incident in the past year, and 4 respondents detecting 3 or more incidents [Q28]. (Compare with 2017, where 12 out of 20 respondents detected at least one incident, and 5 detecting more than 3.) As in previous years, there appears to be a strong distinction between incident "detectors" and non-detectors, with a small number of organizations that detect several incidents, while the majority detect none. This may be due to a "blissful ignorance" effect, where most organizations simply lack the capability (or motivation) to detect most incidents; or possibly due to differing internal definitions for what constitutes an incident.

4.3.13 Of the 9 respondents who listed at least one cybersecurity incident, the most commonly identified programmatic impacts caused by those incidents were the interruption of remote access (6), the impact on data integrity (3), and the impact on institutional reputation (3) [Q29]. Respondents identify the compromise and failure of servers as being the largest operational impact of cybersecurity incidents (5) [Q30].

4.4 Cybersecurity Concerns

4.4.1 When asked what would most improve their cybersecurity stature, the most common response was "increased cybersecurity staff" (11), followed by advanced security technologies (9), "senior management commitment" (8), and "larger budget" (7). This is a shift from previous years, where larger budgets tended to be the most popular response.

4.4.2 There was no clear agreement on what the biggest cybersecurity gap was currently, with only improved inventory tools (2) and improved cybersecurity staffing (3) receiving more than one vote.

4.4.3 The most concerning threats respondents face are "unauthorized or accidental modification of data" (13), "unauthorized, malicious network/system access" (10), and "loss of availability or sabotage of systems" (9). Interestingly, "email viruses, ransomware or other malware" was not particularly concerning, with only 3 respondents selecting it (despite being able to select multiple options).

5 Conclusion

This year's survey continued a trend of high responses-rates from NSF Major Facilities, providing valuable insight into the security programs, practices, and concerns of this unique community. We hope that these results and the subsequent analysis provide some benchmarking insight and inspire discussion, particularly for Major Facilities and projects with larger budgets. Looking ahead, Trusted CI will use this report and past community survey reports to fuel discussions and inform its services. Moreover, we will look for community feedback on changes to future surveys to improve its salience to the community.

Although we received too few responses to claim a representative sample of the NSF science community as a whole, the high response rate of Major Facilities provides greater insight this subset of NSF facilities, and the overall dataset should still offer interesting (and sometimes concerning) insights into the state of cybersecurity in the NSF science community. Future surveys will explore options for increasing the response rate of smaller projects, such as the use of an abbreviated survey that smaller projects could more easily respond to.

Appendix A: Survey

NSF Community Cybersecurity Benchmarking Survey

Instructions for completing survey

Please submit only one response per institution, project, or facility. (When in doubt, we encourage you to respond.) Completing the survey may require input from the PI, the IT manager, and/or the person responsible for cybersecurity (if those separate areas of responsibility exist). While answering specific questions is optional, we strongly encourage you to take the time to respond as completely and accurately as possible. If you prefer not to respond or are unable to answer a question for some reason, we ask that you make that explicit (e.g., by using "other:" inputs) and provide your reason. Trusted CI will release results to the community that we believe provide anonymity to the individual project or facility respondents.

1. Is your project or facility an NSF Large Facility (or "Major Facility")?

List of Large/Major Facilities -- https://www.nsf.gov/bfa/lfo/docs/major-facilities-list.pdf

- Yes
- No

2. What is the age of your project?

E.g. 8 years

Project or Facility Budget

If you are unable to answer, please provide a reason in the space provided

3. What is your project or facility's annual budget?

Estimate to 1 or 2 significant digits, e.g., $3M, $500K, $23,000

4. What is your project or facility's annual information technology budget?

Estimate to 1 or 2 significant digits, e.g., $1M, $50K, $23,000

5. What is your project or facility's annual cybersecurity budget?

Estimate to 1 or 2 significant digits, e.g., $0, $50K, $23,000, $1.3M

6. What expenses are included in the cybersecurity budget?

Check all that apply

- Labor
- Hardware devices (e.g. firewalls, scanner, forensic devices)
- Software licenses
- Not Applicable
- Don't Know
- Other

7. Has your organization devoted adequate resources (e.g. budget, personnel, tools) to the cybersecurity program to address risks deemed unacceptable by the organization?

- Yes
- No
- Not sure

Project or Facility Attributes

8. Does your project or facility have a lead role with responsibility to advise and provide services to the organization on cybersecurity matters (e.g., ISO, CSO, CISO)?

- Yes, full-time
- Yes, part-time
- No
- Don't know

9. Approximately how many FTEs are involved with cybersecurity work (programmatic or operational) within your project or facility?

- None
- More than 0 up to .5 FTE
- 0.5 to nearly 1.0 FTE
- 1 to nearly 2 FTE
- 2 to nearly 3 FTE
- 3 to nearly 4 FTE
- 4 FTE or greater
- Don't Know
- Other

10. Do individuals from multiple institutions authenticate to the resources of your project or facility?

- Yes - 2 or 3 institutions
- Yes - more than 3 institutions
- No
- Don't know

11. Does your project or facility develop or maintain software?

- Yes, interpreted languages (e.g. PHP, Python, Ruby, Perl)
- Yes, compiled languages (e.g. C, C++, Rust, Java)
- Yes, both interpreted and compiled languages.
- No.
- Other

12. If you develop or maintain software, what policies, processes or tools do you use?

Check all that apply

- Coding standards
- Source code repositories
- Automated testing
- Continuous Integration
- Static and/or dynamic analysis
- Issue tracking / vulnerability management
- Testing policy (e.g., regression testing of patches)
- Code signing
- Automated documentation tools (e.g., pydoc)
- Not applicable
- Other

Cybersecurity Program

13. Does your project or facility have a cybersecurity program?

A "cybersecurity program" is a structured approach to develop, implement, and maintain a productive organizational environment with appropriate levels of information-related risk.

- Yes
- No, but we are in the process of establishing one
- No, and we have no current plans to establish one
- Not sure

14. For which groups of individuals does your organization have relevant cybersecurity policies?

Check all that apply

- System operators
- System owners
- Leadership
- Third parties/Visitors
- Users
- Vendors
- Other

15. How frequently is your organization's senior leadership (e.g. director, c-suite) engaged in cybersecurity decisionmaking?

- Never
- Yearly
- Quarterly
- Monthly
- Weekly
- Daily
- Other

16. How are cybersecurity policies developed and officially adopted within your project or facility?

Check all that apply

- IT Manager or cybersecurity person is responsible
- A formal governance board or group has been established to authorize the policies
- PI or other project or facility leadership are responsible
- There is no formal authorization or adoption process
- The host institution(s) provide the policies
- Other

17. Which of the following actions does your organization formally take with regard to its cybersecurity policies?

Check all that apply

- Develop and Adopt (e.g. have a formal process for writing policies and making them 'official')
- Explain (e.g. provide employee training on the policy)
- Follow and Enforce (e.g. audit policy compliance and enforce any provisions for noncompliance)
- Revise (e.g. periodically review and update policies)

18. What control (if any) has your organization selected as its baseline control set?

A "baseline control set" is a predetermined set of security controls used as a default for organizations when selecting security controls for their assets. Examples of baseline control sets include: the CIS Controls, the ASD Essential Eight, and FISMA Moderate (via NIST SP 800-53).

- No baseline control set

- CIS Controls
- ASD Essential Eight
- FISMA Low - Baseline
- FISMA Moderate - Baseline
- FISMA High - Baseline
- NIST SP 800-171
- ISO 27002
- CSF Framework Core
- PCI-DSS
- Not sure
- Other

19. What framework or additional guidance (if any) has your project or facility adopted for how cybersecurity is done?

Check all that apply

- NIST Risk Management Framework - http://csrc.nist.gov/groups/SMA/fisma/framework.html
- NIST Cybersecurity Framework
- Trusted CI's Guide - http://trustedci.org/guide/
- ISO (ISO/IEC 27005)
- Open Science Cyber Risk Profile (OSCRP)
- Interoperable Global Trust Federation (IGTF)
- The parent institution is responsible for the framework
- None
- Other

20. Does your organization have a process for selecting and deploying "additional controls"?

"Additional controls" are controls selected beyond those specified in the baseline control set. Reasons for selecting an additional control include: to address a particularized threat; to address an unacceptable risk; to satisfy a compliance requirement; or to satisfy a contractual obligation.

- Yes
- No
- Not sure

21. Does your organization have a process for selecting and deploying "alternate controls"?

"Alternate controls" are those selected instead of controls in the baseline control set. Reasons for selecting an alternate control in place of a baseline control include: improves employee quality of life; better addresses the organization's operating environment; better addresses the organization's unique risk profile; or the baseline control was too costly to implement.

- Yes
- No
- Not sure

22. Who accepts residual cybersecurity risk (i.e., the remaining risk after reasonable cybersecurity controls are established)?

Check all that apply

- A cybersecurity person
- IT manager
- System or process owner
- Senior managers or PI

- An individual in the parent institution (external to the project)
- No one / there is no explicit risk acceptance process
- Don't Know
- Other

23. What external cybersecurity requirements (if any) are imposed on your project or facility?

Check all that apply

- State or federally protected Personally Identifiable Information (PII)
- Protected Health Information (PHI)
- Non-disclosure or contractual agreements (NDA)
- Classified information - https://en.wikipedia.org/wiki/Classified_information_in_the_United_States
- FISMA / NIST RMF
- NIST CSF
- CUI / NIST SP 800-171
- Cooperative agreement terms from NSF
- None
- Don't know
- Other

24. What kind(s) of identity management does your project or facility employ to control access to its resources?

Check all that apply

- The parent institution's identity management
- Separately maintained project or facility userid/password
- Independent project or facility certificate-based infrastructure
- Federated identity management technology
- Other

25. What programmatic cybersecurity safeguards has your project or facility implemented?

Check all that apply

- Utilize cybersecurity maturity model to assess and/or plan program evolution
- Have an overarching cybersecurity strategy, policy or plan
- Have a roadmap for cybersecurity improvements
- Have documented cybersecurity standards/baselines for employees and/or external researchers
- Inventory critical information assets
- Have a data classification scheme
- Have a cyber incident response plan
- Have business continuity/disaster recovery plans
- Require periodic cybersecurity awareness training for personnel
- Conduct risk assessments
- Monitor/analyze security intelligence
- Have an Information Security governance structure
- Conduct review by external organizations
- Utilize programmatic safeguards of parent institution
- None
- Other

26. What operational cybersecurity safeguards has your project or facility implemented?

Check all that apply

- Multi-Factor Authentication

- Centralized logging system
- Vulnerability management
- Scan for vulnerabilities or configuration errors
- Physical access controls to critical resources
- Intrusion Detection Systems / Intrusion Prevention System
- Network firewalls that block all but required access ports / protocols
- Anti-virus / Anti-spam / spyware / phishing solutions
- Data loss prevention / file encryption
- Real-time alerting of possible attacks / anomalies
- Internal tabletop exercises to gauge organizational response
- Live cybersecurity exercises
- Penetration or phishing tests
- Utilize operational safeguards of parent institution
- None
- Other

27. How frequently are patches applied based on the severity rating, either on a fixed maintenance cycle (e.g., monthly) or based on some regular cycle after a patch is released?

Choose a single value for each row. If multiple values are appropriate depending on system type, choose the shortest interval.

	2 Days	1 Week	1 Month	3 Months	> 3 Months
Critical					
Important					
Moderate					
Low					

28. How many cybersecurity incidents (i.e., any event that puts the confidentiality, integrity, or availability of data or information systems at risk) has your project or facility experienced in the past year?

- 1
- 2
- 3
- >3
- None
- Don't know
- Prefer not to answer

29. For the cybersecurity incidents your project or facility experienced in the past year, what were the programmatic impacts?

Check all that apply

- Loss of reputation
- Decreased confidence in data integrity
- Temporary or permanent inability to collect or analyze data
- Interruption of remote access
- Sanctions or legal actions due to breach of sensitive information
- Significant cost of incident recovery procedures
- Cost of additional remediation procedures / controls
- Does not apply

- Other

30. For the cybersecurity incidents your project or facility experienced in the past year, which have had the greatest operational impact?

Check no more than 2

- Network denial of service
- Compromise / failure of servers
- Compromise or infection of workstations
- Compromised / lost / stolen portable devices (mobile phones, laptops)
- Theft or alteration of data (e.g. password files, HIPAA, PII, NDA, prepublication results)
- No detected incidents
- Other

Cybersecurity Concerns

31. What would most improve your project or facility's cybersecurity stature?

Check at most 2

- Advanced security technology (hardware and/or software)
- Cybersecurity steering committee
- Employee/researcher reward / disciplinary systems
- Increased cybersecurity staff
- Larger cybersecurity budget
- Senior Management commitment
- Other

32. What cybersecurity threats are of most concern to your project or facility?

Check at most 2

- Unauthorized or accidental modification of data
- Exposure of confidential or sensitive information
- Loss of availability or sabotage of systems
- Incorrect network/hardware/software configurations
- Email viruses, ransomware or other malware
- Unauthorized, malicious network/system access
- Other

33. What external cybersecurity services or community resources does your organization utilize?

External cybersecurity services include: incident response; security as a service providers; third party network monitoring; third party audits; and third party training services.

34. What external cybersecurity tools does your organization utilize?

External cybersecurity tools include: network monitoring tools; secure configuration management tools; and asset inventory tools.

35. What are the cybersecurity needs and/or gaps you are currently experiencing or expect in the next three years?

36. Comments - Use this space to record any additional or clarifying comments.

Feedback

Thank you for your participation in the Trusted CI Community Survey. If you have any feedback, please feel free to add comments below.